IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appellant: Lu, et al.	§	
	§	Group Art Unit: 2444
Application No.: 10/593,314	§	
	§	Examiner: Farrukh Hussain
§ 371(c) Date: April 17, 2007	§	
	§	Confirmation No.: 7532
For: METHOD FOR BINDING WORK LABEL SWITCHING PATH AND PROTECTION LABEL SWITCHING PATH	§	
	§	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

CERTIFICATE OF EFS-WEB FILING

Pursuant to 37 C.F.R. §1.8, I hereby certify that this correspondence is being electronically submitted to the U.S. Patent and Trademark Office website, www.uspto.gov, on

June 24, 2011

Jerri Pearson

Jerri Pearson

REPLY BRIEF

Dear Sirs:

This Reply Brief is filed in support of the appeal in the above-referenced application and is filed pursuant to the Notice of Appeal filed February 3, 2011, the Appeal Brief filed February 15, 2011, and the Examiner's Answer dated April 26, 2011. The Appellant authorizes all required fees under 37 C.F.R. § 1.17 to be charged to Deposit Account No. 50-1515, of Conley Rose, P.C. of Texas.

TABLE OF CONTENTS

I. STATUS OF CLAIMS

A. Total Number of Claims in the Application

Claims in the application: 1-19.

B. Status of All Claims in the Application

1. Claims canceled: None.

2. Claims withdrawn from consideration but not canceled: None.

3. Claims pending: 1-19.

4. Claims allowed: None.

6. Claims objected to: None.

5. Claims rejected: 1-19.

C. Claims on Appeal

Claims on appeal: 1-19.

II. GROUNDS FOR REJECTION TO BE REVIEWED ON APPEAL

1. Whether claims 1-19 are rendered obvious under 35 U.S.C. § 103(a) by the combination of U.S. Patent Application Publication 2004/0004955 (*Lewis*), U.S. Patent Application Publication 2002/0116669 (*Jain*), and U.S. Patent 7,315,510 (*Owens*).

III. ARGUMENTS

A. The combination of *Lewis, Jain,* and *Owens* fails to render obvious claims 1-19 because the combination of *Lewis, Jain,* and *Owens* fails to disclose that the PML router assigns a label for the protection LSP based on a message requesting creation of the protection LSP for the work LSP.

The combination of *Lewis, Jain,* and *Owens* fails to render obvious claims 1-19 because the combination of *Lewis, Jain,* and *Owens* fails to disclose that the PML router assigns a label for the protection LSP based on a message requesting creation of the protection LSP for the work LSP. Claims 1 and 3 read:

> 1. A method for binding a work label switching path (LSP) with a protection LSP, comprising:
>
> **a Path Switching Label Switching Router (PSL) transmitting a first message** which comprises a binding information to a Path Merging Label Switching Router (PML) **to request for creating the protection LSP of the work LSP**;
>
> **the PML router assigning a label for the protection LSP based on the first message**, and returning a second message which comprises the binding information;
>
> upon receiving the second message, the PSL router binding the work LSP with the protection LSP according to the binding information, and transmitting a notification message which comprises the binding information to the PML switched router; and
>
> the PML router binding the work LSP with the protection LSP according to the binding information in the notification message,
>
> wherein the binding information comprises an identifier of the work LSP, a type of the LSP, and a protection mode, and
>
> wherein the PSL and PML are label edge routers.

> 3. A method for binding a work label switching path (LSP) with a protection LSP, comprising:
>
> in the process of creating the protection LSP, **a Path Switching Label Switching Router (PSL) transmitting a first message** which comprises a binding information to a Path Merging Label Switching Router (PML) **to request for creating the protection LSP of the work LSP**;
>
> **the PML router assigning a label for the protection LSP based on the first message**, and returning a second message which comprises the binding information;
>
> upon receiving the second message, the PSL router binding the work LSP with the protection LSP according to the binding information, and transmitting a notification message which comprises the binding information to the PML switched router; and
>
> the PML router binding the work LSP with the protection LSP according to the binding information in the notification message,
>
> if the protection mode for the work LSPs is 1+1 mode, the binding information comprises the work LSP identifier, LSP type, and the protection mode; and
>
> if the protection mode for the work LSPs is 1:1, the binding information comprises the work LSP identifier, LSP type, the protection mode and selection mode of the return LSP in the 1:1 protection mode.

(Emphasis added). As shown above, claims 1 and 3 require that the PML router assigns a label for the protection LSP **based on a message requesting creation of the protection LSP for the work LSP**. The Examiner asserts that *Owens's* col. 1, ll. 40-46, and col. 4, ll. 32-67 discloses that the PML router assigns a label for the protection LSP based on a message requesting creation of the protection LSP for the work LSP. *See* Examiner's Answer dated April 26, 2011 (*Examiner's Answer*), p. 19-20. However, the cited portion of *Owens* is concerned with rerouting data over existing protection paths, rather than with assigning a label to a protection path during the process of creating the protection path.[1] Specifically, the cited portion of *Owens* assigns labels to **IP packets** to reroute the packets over an existing protection path based upon an affirmative notice message (i.e. a message indicating a pathway failure), but does not assign a label to the **protection LSP** based upon a message requesting creation of the protection LSP:

[1] *See* Claim 1, *supra*, ("**in the process of creating the protection LSP**, a Path Switching Label Switching Router (PSL) transmit[s] a first message [and] the PML router assign[s] a label for the protection LSP based on the first message").

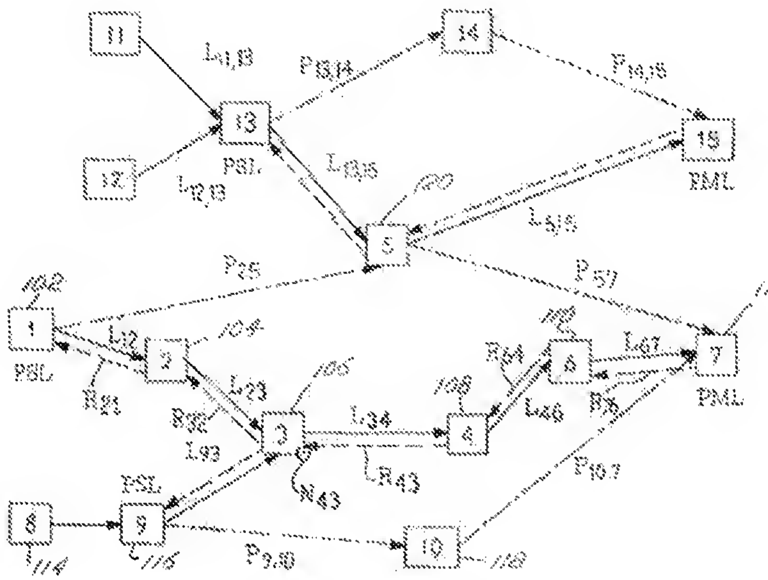
> The key concept in MPLS is **identifying and marking IP packets with labels and forwarding them to a modified switch or router**, which then uses the labels to switch the packets through the network. **The labels are created and assigned to IP packets based upon the information gathered from existing IP routing protocols.**
>
> Multi-protocol label switching (MPLS) networks are typically comprised of several packet-based switching systems interconnected by a variety of media (e.g., coaxial or fiber optic cable, unshielded twisted pair or even point-to-point microwave wireless) in a mesh-topology network similar to the public switched telephone network. In such a network, there might be several paths through the network between any two endpoints. **MPLS networks carry data as packets wherein each packet includes a label on identifying a switched path through the network. The data label is appended to data packets so as to define a pathway through the network over which the data packets are to be routed**.
>
> **In the event of a pathway failure** causing downstream data to be lost at a downstream switch, such as by either a switch failure or a link failure, anywhere along a primary or working path, **a protection switch element (PSL), such as switch no. 1 (identified by reference numeral 102) can re-route data traffic through the protection path** so as to have the data for the endpoint switch no. 7 delivered as quickly as possible to the endpoint at switch no. 7 (identified by reference numeral 112). **The ability to re-route data to a protection path is made considerably more valuable if the decision to switch over to a protection path is based upon an affirmative notice that a switch over is needed. In one embodiment, this affirmative notice is in the form of an upstream liveness message, the loss of which indicates a pathway failure**. As long as a liveness message is received at an upstream switch from a downstream switch, the upstream switch can assume that the pathway between the two switches is intact and that the downstream switch is functional.

Owens, col. 1, ll. 40-46, col. 1, l. 65 – col. 2, l. 9, and col. 4, l. 55 - col. 5, l. 6 (emphasis added). As shown above, *Owens* assigns a label to IP packets to define the pathway over which the IP packets are to be routed through the network. Further and as shown above, *Owens's* protection switch element (PSL) assigns a label to IP packets (rather than to a protection path) upon receiving a message indicating a failure in the working path (rather than a message requesting creation of the protection path).

The Examiner further asserts that *Owens*'s PSL is a protection LSP that is created by an affirmative notice (request). *See Examiner's Answer*, p. 20. The Appellants respectfully

disagree for three reasons. First, *Owens's* affirmative notice message **requests a switch over to an existing protection LSP**, but does not request the creation of a protection LSP. *See Owens*, col. 4, ll. 63-66, *supra* ("The ability to re-route data to a protection path is made considerably more valuable if the decision to switch over to a protection path is based upon an affirmative notice that a switch over is needed.") (Emphasis added). Second, *Owens's* PSL element is a network node, not a protection path:

FIG. 1



> In the event of a pathway failure causing downstream data to be lost at a downstream switch, such as by either a switch failure or a link failure, anywhere along a primary or working path, **a protection switch element (PSL), such as switch no. 1 (identified by reference numeral 102) can re-route data traffic through the protection path** so as to have the data for the endpoint switch no. 7 delivered as quickly as possible to the endpoint at switch no. 7 (identified by reference numeral 112). The ability to re-route data to a protection path is made considerably more valuable if the decision to switch over to a protection path is based upon an affirmative notice that a switch over is needed. In one embodiment, this affirmative notice is in the form of an upstream liveness message, the loss of which indicates a pathway failure. As long as a liveness message is received at an upstream switch from a downstream switch, the upstream switch can assume that the pathway between the two switches is intact and that the downstream switch is functional.

Owens, col. 4, l. 55 – col. 5, l. 6 (emphasis added). As shown above in FIG. 1, *Owens's* PSL 102 is a network node, not a protection path. Third, *Owens's* PSL 102 receives the affirmative notice message, and therefore cannot be created by the affirmative notice message.

> In the event of a pathway failure causing downstream data to be lost at a downstream switch, such as by either a switch failure or a link failure, anywhere along a primary or working path, **a protection switch element (PSL), such as switch no. 1 (identified by reference numeral 102) can re-route data traffic through the protection path** so as to have the data for the endpoint switch no. 7 delivered as quickly as possible to the endpoint at switch no. 7 (identified by reference numeral 112). **The ability to re-route data to a protection path is made considerably more valuable if the decision to switch over to a protection path is based upon an affirmative notice that a switch over is needed**. In one embodiment, this affirmative notice is in the form of an upstream liveness message, the loss of which indicates a pathway failure. As long as a liveness message is received at an upstream switch from a downstream switch, the upstream switch can assume that the pathway between the two switches is intact and that the downstream switch is functional.

Owens, col. 4, l. 55 – col. 5, l. 6 (emphasis added). As shown above, *Owens's* PSL makes the decision to re-route the traffic over the protection path upon receiving the affirmative notice message indicating that a switch over is needed. Hence, *Owens's* PSL receives the affirmative notice message, and therefore cannot be created by the affirmative notice message. Thus, *Owens* fails to disclose that the PML router assigns a label for the protection LSP based on a message requesting creation of the protection LSP for the work LSP. *Lewis* fails to make up for the deficiencies of *Jain* and *Owens*. Therefore, the combination of *Lewis, Jain*, and *Owens* fails to disclose that the PML router assigns a label for the protection LSP based on a message requesting creation of the protection LSP for the work LSP. As such, the combination of *Lewis, Jain*, and *Owen* fails to disclose at least one limitation of independent claims 1 and 3, and consequently fails to render obvious claims 1-19.

B. The combination of *Lewis, Jain,* and *Owens* fails to render obvious claims 1-19 because the combination of *Lewis, Jain,* and *Owens* fails to disclose that a first message sent from the PSL to the PML, a second message sent from the PML to the PSL, and a notification message sent from the PSL to the PML all comprise an identifier of the work LSP.

The combination of *Lewis, Jain,* and *Owens* fails to render obvious claims 1-19 because the combination of *Lewis, Jain,* and *Owens* fails to disclose that a first message sent from the PSL to the PML, a second message sent from the PML to the PSL, and a notification message sent from the PSL to the PML all comprise an identifier of the work LSP. Claims 1 and 3 read:

> 1. A method for binding a work label switching path (LSP) with a protection LSP, comprising:
>
> **a Path Switching Label Switching Router (PSL) transmitting a first message which comprises a binding information to a Path Merging Label Switching Router (PML)** to request for creating the protection LSP of the work LSP;
>
> **the PML router** assigning a label for the protection LSP based on the first message, and **returning a second message which comprises the binding information**;
>
> upon receiving the second message, **the PSL router** binding the work LSP with the protection LSP according to the binding information, and **transmitting a notification message which comprises the binding information to the PML switched router**; and
>
> the PML router binding the work LSP with the protection LSP according to the binding information in the notification message,
>
> **wherein the binding information comprises an identifier of the work LSP**, a type of the LSP, and a protection mode, and
>
> wherein the PSL and PML are label edge routers.

3. A method for binding a work label switching path (LSP) with a protection LSP, comprising:

in the process of creating the protection LSP, **a Path Switching Label Switching Router (PSL) transmitting a first message which comprises a binding information to a Path Merging Label Switching Router (PML)** to request for creating the protection LSP of the work LSP;

the PML router assigning a label for the protection LSP based on the first message, and **returning a second message which comprises the binding information**;

upon receiving the second message, **the PSL** router binding the work LSP with the protection LSP according to the binding information, and **transmitting a notification message which comprises the binding information to the PML switched router**; and

the PML router binding the work LSP with the protection LSP according to the binding information in the notification message,

if the protection mode for the work LSPs is 1+1 mode, **the binding information comprises the work LSP identifier**, LSP type, and the protection mode; and

if the protection mode for the work LSPs is 1:1, **the binding information comprises the work LSP identifier**, LSP type, the protection mode and selection mode of the return LSP in the 1:1 protection mode.

(Emphasis added). As shown above, claims 1 and 3 require that a first message sent from the PSL to the PML, a second message sent from the PML to the PSL, and a notification message sent from the PSL to the PML all comprise an identifier of the work LSP. The Examiner asserts that *Lewis's* ¶¶ 7, 9, and 44 disclose that a first message sent from the PSL to the PML, a second message sent from the PML to the PSL, and a notification message sent from the PSL to the PML all comprise an identifier of the work LSP. *See Examiner's Answer*, p. 20. The Appellants respectfully disagree with the Examiner's contention for at least two reasons. First, *Lewis's* error notification message is not exchanged between the same two nodes as the first and the second LSP setup requests, as required by claims 1 and 3.[2] Specifically, *Lewis's* first and second LSP setup requests are exchanged between the two label end routers (LERs), i.e., between LER 106

[2] Claims 1 and 3 require a first message from the PSL to the PML, a second message from the PML to the PSL, and a notification message transmitted from the PSL to the PML. Hence, claim 1 and 3 require that each of the first message, the second message, and the notification message be exchanged between **the same two network devices** (i.e. between the PSL and the PML).

and LER 110, while *Lewis's* error notification message is sent from an intermediate transit router, i.e., the label switched router (LSR) 108, to the first LER:

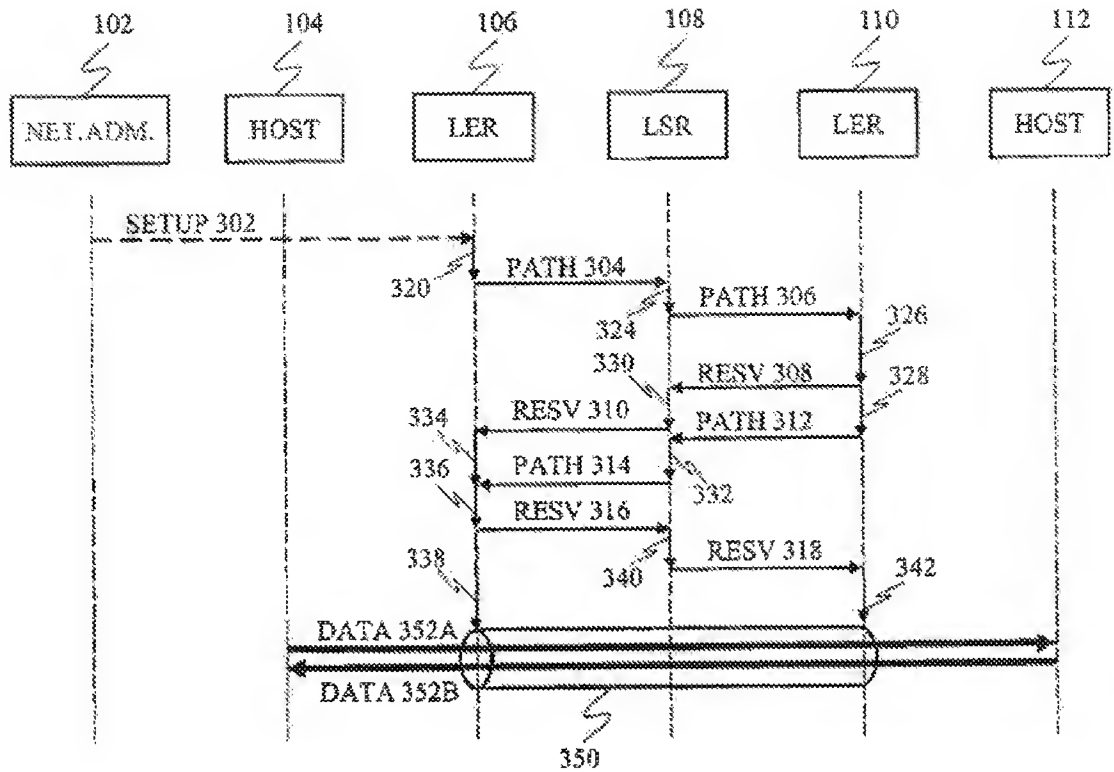


FIG. 3

The problems experienced in constructing bi-directional label switched paths are overcome by the present invention, in its several embodiments including a method and an apparatus for automatically establishing a complementary label switched path. **The method of forming a bi-directional LSP between a first and second routing device is comprised of the steps of: sending a first LSP setup request message comprising a first bi-directional indicator from the first routing device to the second routing device; and automatically sending a second LSP setup request message from the second routing device to the first routing device** in response to the first bi-direction indicator; wherein a first unidirectional LSP is established in a message exchange initiated by the first LSP setup request message, and a second unidirectional label switched path is established in a message exchange initiated by the second LSP setup request message.

> In some embodiments, **the first and second LSP setup request messages are first and second RSVP PATH messages**, respectively, used to request resources from the endpoint routers and the transit routers. The first and second RSVP PATH messages preferably invoke first and second RSVP RESV messages, respectively, that consummate the reservation of the resources at the various routers and established the label convention used by data that is subsequently transmitted from the endpoint routers.
>
> In some embodiments, the first and second LSP setup request messages include opaque objects that signal the formation of the bi-directional LSPs between endpoints. The first LSP setup request message preferably includes a first bi-direction indicator that uniquely identifies the LSP and specifies the resource requirements of the return LSP. The second LSP setup request message is automatically generated at the receiving LER in response to the first bi-direction indicator. The second LSP setup request message preferably includes a second bi-directional indicator that indicates to the original LER that the second of the two unidirectional LSPs may be associated at the endpoints once the return LSP is created. In the preferred embodiment, the first and second LSP setup request messages are RSVP PATH messages that are followed by RSVP RESV messages.
>
> The treatment of the RESV message 308 in the preferred embodiment is consistent with that prescribed in the RSVP standard. The RESV message 308 is forwarded towards the LER 106 along the same route of the first LSP path message. Upon receipt, the transit router 108 looks into the message 308 to determine if it has sufficient available resources to provide the bandwidth and QOS requested in the previous PATH message 304 for the forward LSP. If available, the transit router 108 updates its MPLS forwarding table with the MPLS label from the LER 110 and outgoing port number included in the RESV message 308. **If the check fails for lack of available resources, for example, transit router 108 returns an error notification to the LER 110 that made the initial request.**

Lewis, FIG. 3 and ¶¶ 7-9 and 44 (emphasis added). As shown above, *Lewis's* first LSP setup message (i.e. path message 304/306) is sent from the LER 106 to the LER 110 and *Lewis's* second LSP setup message (i.e. the path message 312/314) is sent from the LER 110 to the LER 106. Hence, *Lewis's* first and second path messages are exchanged between **the LER 106 and the LER 110**. However, *Lewis's* error notification message is sent from the transit router 108 (i.e. the LSP 108) to the LER 110, and therefore is exchanged between the LSP 108 and the LER 110 (rather than between the LER 106 and the LER 110). Consequently, *Lewis's* error

notification message is not exchanged between the same two nodes as the first and the second LSP setup requests. Second, *Lewis's* error notification does not comprise an identifier of the work LSP:

> The treatment of the RESV message 308 in the preferred embodiment is consistent with that prescribed in the RSVP standard. The RESV message 308 is forwarded towards the LER 106 along the same route of the first LSP path message. Upon receipt, the transit router 108 looks into the message 308 to determine if it has sufficient available resources to provide the bandwidth and QOS requested in the previous PATH message 304 for the forward LSP. If available, the transit router 108 updates its MPLS forwarding table with the MPLS label from the LER 110 and outgoing port number included in the RESV message 308. **If the check fails for lack of available resources, for example, transit router 108 returns an error notification to the LER 110 that made the initial request**.

Lewis, ¶ 44. As shown above, *Lewis's* error notification indicates that a check has failed for lack of available resources, but does not comprise an identifier of the work LSP. *Jain* fails to make up for the shortcomings in *Lewis* and *Owens*. As such, the combination of *Lewis*, *Jain*, and *Owens* fails to disclose at least one limitation of claims 1 and 3, and consequently fails to render obvious claims 1-19.

C. The combination of *Lewis, Jain*, and *Owens* fails to render obvious claims 1-19 because the combination of *Lewis, Jain*, and *Owens* fails to disclose that a first message sent from the PSL to the PML, a second message sent from the PML to the PSL, and a notification message sent from the PSL to the PML all comprise the type of LSP.

The combination of *Lewis*, *Jain*, and *Owens* fails to render obvious claims 1-19 because the combination of *Lewis*, *Jain*, and *Owens* fails to disclose that a first message sent from the PSL to the PML, a second message sent from the PML to the PSL, and a notification message sent from the PSL to the PML all comprise the type of LSP. Claims 1 and 3 read:

1. A method for binding a work label switching path (LSP) with a protection LSP, comprising:

a Path Switching Label Switching Router (PSL) transmitting a first message which comprises a binding information to a Path Merging Label Switching Router (PML) to request for creating the protection LSP of the work LSP;

the PML router assigning a label for the protection LSP based on the first message, and **returning a second message which comprises the binding information**;

upon receiving the second message, **the PSL router** binding the work LSP with the protection LSP according to the binding information, and **transmitting a notification message which comprises the binding information to the PML switched router**; and

the PML router binding the work LSP with the protection LSP according to the binding information in the notification message,

wherein the binding information comprises an identifier of the work LSP, **a type of the LSP**, and a protection mode, and

wherein the PSL and PML are label edge routers.

3. A method for binding a work label switching path (LSP) with a protection LSP, comprising:

in the process of creating the protection LSP, **a Path Switching Label Switching Router (PSL) transmitting a first message which comprises a binding information to a Path Merging Label Switching Router (PML)** to request for creating the protection LSP of the work LSP;

the PML router assigning a label for the protection LSP based on the first message, and **returning a second message which comprises the binding information**;

upon receiving the second message, **the PSL** router binding the work LSP with the protection LSP according to the binding information, and **transmitting a notification message which comprises the binding information to the PML switched router**; and

the PML router binding the work LSP with the protection LSP according to the binding information in the notification message,

if the protection mode for the work LSPs is 1+1 mode, **the binding information comprises the** work LSP identifier, **LSP type**, and the protection mode; and

if the protection mode for the work LSPs is 1:1, **the binding information comprises** the work LSP identifier, **LSP type**, the protection mode and selection mode of the return LSP in the 1:1 protection mode.

(Emphasis added). As shown above, claims 1 and 3 require that a first message sent from the PSL to the PML, a second message sent from the PML to the PSL, and a notification message sent from the PSL to the PML **all comprise the type of LSP**. The Examiner asserts that *Lewis's*

¶¶ 7, 9, and 44 discloses a first message sent from the PSL to the PML, a second message sent from the PML to the PSL, and a notification message sent from the PSL to the PML, and that *Owens's* col. 9, ll. 40-52 discloses a message comprising a type of LSP. *See Examiner's Answer*, p. 22. The Appellants respectfully disagree with the Examiner's assertion for at least two reasons. First and as discussed above, *Lewis's* error notification message is not exchanged between the same two nodes as the first and the second LSP setup requests. Therefore, *Lewis* does not disclose that a first message sent from the PSL to the PML, a second message sent from the PML to the PSL, and a notification message sent from the PSL to the PML. Second, *Owens's* col. 9, ll. 40-52 discloses an LSP that requires signaling between a protection switch element (such as a router) and destination switch (another router), but <u>fails to disclose that a message comprises an LSP type</u>:

> The RNT is rooted at an appropriately chosen label switched router ("LSR"), (which hereafter is referred to as an MPLS network switch element) along the common segment of the merged working paths and is terminated at the protection switch elements (PSLs). Intermediate network switching elements on the converged working paths typically share the same RNT reducing signaling overhead associated with recovery. Unlike schemes that treat <u>**each label switched path (LSP) independently, and require signaling between a protection switch element and a destination switch individually for each LSP**</u>, the RNT allows for only one (or a small number of) signaling messages on the shared segments of the LSPs.

Owens, col. 9, ll. 40-52 (emphasis added). As shown above, the cited portion of *Owens* discloses an LSP that requires signaling between a protection switch element (such as a router) and destination switch (another router), but does not disclose a message comprising an LSP type. Thus, *Lewis* and *Owens*, neither alone nor in combination, disclose that a first message sent from the PSL to the PML, a second message sent from the PML to the PSL, and a notification message sent from the PSL to the PML all comprise the type of LSP. *Jain* fails to make up for the shortcomings in *Owens*. As such, the combination of *Lewis*, *Jain*, and *Owens* fails to

disclose at least one limitation of claims 1 and 3, and consequently fails to render obvious claims 1-19.

D. The combination of *Lewis, Jain,* and *Owens* fails to render obvious claims 2 and 9-14 because the combination of *Lewis, Jain,* and *Owens* fails to disclose designating the protection mode of the work LSP at the PSL switched router.

In addition to the reasons provided above, the combination of *Lewis, Jain,* and *Owens* fails to render obvious claims 2 and 9-14 because the combination of *Lewis, Jain,* and *Owens* fails to disclose designating the protection mode of the work LSP at the PSL switched router. Claim 2 reads:

> 2. The method according to claim 1, further comprising: before creating the work LSP, **designating the PML router and the protection mode of the work LSPs at the PSL switched router**; or, after creating the work LSP, **designating the PML router and the protection mode of the work LSPs at the PSL switched router**.

(Emphasis added). As shown above, claim 2 requires **designating the protection mode of the work LSP at the PSL switched router**. The Examiner contends that *Jain's* ¶¶ 13 and 106 disclose designating the protection mode of the work LSPs at the PSL switched router. *See Examiner Answer*, p. 23. However, while the cited portions of *Jain* may discuss various protection modes (e.g. 1+1, 1:n, or 1:1 protection types), the cited portions of *Jain* do not disclose that the protection mode for the work LSP is **designated at the PSL router**:

> Each router may then store the SRLGs that relate to its own possible points of failure and those that relate to possible points of failure in other portions of the network. For example, each router may store only the SRLGs that correspond to resources within the network that the particular router is using to send data, e.g., those resources being used by label-switched paths (LSPs) set up by that router.

> Then, program flow moves to a state 906 in which a level or type of protection criteria for the resource identified in the state 904 may be specified. This criteria may, for example, specify a level of redundancy available to the resource. **The level or kind of criteria specified in the state 906 will generally result from the topology of the network and from characteristics of individual network elements.** For example, the protection provided may be 1:1, 1:n, 1+1, ring, or fast re-route. Fast re-route may be as explained above in reference to FIGS. 6-8 or another fast re-routing technique. Further, these criteria may be further specified according to classes and sub-classes of protection. For example, 1:1 protection may be considered a special case of 1:n protection that provides a higher level of fault tolerance than other 1:n levels.

Jain, ¶¶ 13 & 106 (emphasis added). As shown above, *Jain* discusses various protection modes (e.g. 1+1, 1:n, or 1:1 protection types), but does not disclose that the protection mode of the work LSP **is designated at the PSL switched router**. *Lewis* and *Owens* fail to make up for the deficiencies of *Jain*. Thus, the combination of *Lewis*, *Jain*, and *Owens* fails to disclose designating the protection mode of the work LSP at the PSL switched router. As such, the combination of *Lewis*, *Jain*, and *Owens* fails to disclose all of the elements of claims 2, and consequently, fails to render obvious claims 2 and 9-14.

E. The combination of *Lewis*, *Jain*, and *Owens* fails to render obvious claims 10-14 because *Jain* fails to disclose that the steps for creating the return LSP are performed after the PML router receives the notification message.

In addition to the reasons provided above, the combination of *Lewis*, *Jain*, and *Owens* fails to render obvious claims 10-14 because the combination of *Lewis*, *Jain*, and *Owens* fails to disclose that the steps for creating the return LSP are performed after the PML router receives the notification message. Claim 10 reads:

> 10. The method according to claim 9, **after the PML router receives the notification message,** if it is determined that the protection is in the 1:1 mode and it is chosen to create the return LSP dynamically via signaling, further comprising:
>
> the PML router transmitting to the PSL router a third message of requesting for creating the return LSP, with the binding information included in the third message;
>
> the PSL router assigning a label for the return LSP according to the third message, and returning a fourth message which comprises the binding information;
>
> the PML router binding the work LSP and the return LSP based on the binding information of the fourth message, and transmitting to the PSL router a notification message which comprises the binding information; the PSL router binding the work LSP and the return LSP based on the binding information of the notification message.

(Emphasis added). As shown above, claim 10 requires that the steps[3] for creating the return LSP are performed **after the PML router receives the notification**. The Examiner contends that *Jain's* ¶ 15 discloses that the steps in claim 10 are performed after the PML router receives the notification. *See Examiner's Answer*, p. 24. However, the cited portions of *Jain* disclose propagating a notification to other nodes in the network after receiving the notification message, but do not disclose performing the steps for creating a return LSP after receiving the notification message:

> When the neighboring routers receive the notification, they each take notice of the failure. In addition, **the neighboring routers may propagate the notification to other nodes in the network**. Thus, in a short time, each router in the network is notified of the failure and records the failed network resource identified by the SRLG that is contained in the original failure notification.

Jain, ¶ 15 (emphasis added). As shown above, *Jain* propagates the notification throughout the network after the notification is received, but does not create a return LSP after the notification is received. *Lewis* and *Owens* fail to make up for the shortcomings in *Jain*. Thus, the combination of *Lewis*, *Jain*, and *Owens* fails to disclose that the steps for creating the return LSP are

[3] The steps for creating the return LSP include "requesting creat[ion] [of] the return LSP", "assigning a label for the return LSP", "binding the work LSP and the return LSP [by the PML]", "transmitting ... a notification message which comprises the binding information", and "binding the work LSP and the return LSP [by the PSL]".

performed after the PML router receives the notification. As such, the combination of *Lewis*, *Jain*, and *Owens* fails to disclose all of the elements of claim 10, and consequently, fails to render obvious claims 10-14.

F. The combination of *Lewis, Jain*, and *Owens* fails to render obvious claims 10-14 because the combination of *Lewis, Jain*, and *Owens* fails to disclose that the notification message comprises binding information.

In addition to the reasons provided above, the combination of *Lewis*, *Jain*, and *Owens* fails to render obvious claims 10-14 because the combination of *Lewis*, *Jain*, and *Owens* fails to disclose that the notification message comprises binding information. Claim 10 reads:

> 10. The method according to claim 9, after the PML router receives the notification message, if it is determined that the protection is in the 1:1 mode and it is chosen to create the return LSP dynamically via signaling, further comprising:
>
> the PML router transmitting to the PSL router a third message of requesting for creating the return LSP, with **the binding information included in the third message**;
>
> the PSL router assigning a label for the return LSP according to the third message, and returning **a fourth message which comprises the binding information**;
>
> the PML router binding the work LSP and the return LSP based on the binding information of the fourth message, and transmitting to the PSL router **a notification message which comprises the binding information**; the PSL router binding the work LSP and the return LSP based on the binding information of the notification message.

(Emphasis added). As shown above, claim 10 requires that the notification message comprises binding information. The Examiner contends that *Owens's* col. 5, ll. 25-34 and col. 11, ll. 1-31 disclose that the notification message comprises binding information. *See Examiner's Answer*, p. 24. However, the cited sections of *Owens* do not disclose that the notification message comprises binding information:

> Those skilled in the art will appreciate that while the loss of a liveness message can trigger a protection switch of data to a protection path, an equivalent alternate embodiment of the invention includes a method by which a protection switchover **is initiated or occurs upon the receipt of either a liveness message or a notification message to a protection switch element**. In such a case, the liveness message and/or the notification acts as a trigger event to cause information to be re-routed onto the protection path.
>
> **Protection Path Establishment**
> A Protection Domain Path is established by the identification of a protection switch or node and an end point switch or node in the MPLS network. The protection switch element ("PSL") initiates the setup of the working LSP and elements and the recovery LSP and elements. It is also responsible for storing information about which network switch elements or portions thereof have protection enabled, and for maintaining a binding between outgoing labels specifying the working path and the protection/recovery path. The latter enables the switchover to the recovery path upon the receipt of a protection switch trigger.
>
> A "label distribution protocol" is a set of procedures by which one LSR (i.e., a network switch element) informs another of the label bindings it has made. "Label binding" is a process by which a message to be sent from a source to a destination is associated with various labels between the nodes that lie along the way, between the source and destination. By way of example, in FIG. 1, a message to be sent from switch 1 to switch 7 is associated or bound to travel to switch 7 through switch 2 by, or using, the label L_{12} that is first associated with the message at, or by, switch 1. Switch 2 in turn associates messages labeled L_{12} as bound for switch 3 and re-labels them as L_{23}. Re-labeling messages (e.g. re-labeling a message received at switch 2 on L_{12}, as the same message that is output from switch 2 but on L_{23} and which is received at switch 3, to be re-labeled by switch 3 and output again as L_{34}) is known as "label binding." **Two or more LSRs, (network switch elements) which use a label distribution protocol to exchange label binding information are known as "label distribution peers" with respect to the binding information they exchange**.

Owens, col. 5, ll. 26-34 and col. 11, l-31. As shown above, *Owens's* binding information is contained in the label distribution protocol messages, which are used to communicate label bindings during the creation of the protection LSP. Importantly, *Owens's* notification messages are not label distribution protocol messages. Specifically, *Owens's* notification messages are exchanged **after** the protection path has been established (e.g. to indicate a switch to the protection path in the event of a failure of the work LSP), while the label distribution protocol

messages are, by definition, exchanged **during** the creation of the protection path. *Lewis* and *Jain* fail to make up for the shortcomings of *Owens*. Thus, the combination *Lewis*, *Jain*, and *Owens* fails to disclose that the notification message comprises binding information. As such, the combination of *Lewis*, *Jain*, and *Owens* fails to disclose all of the elements of claim 10, and consequently, fails to render obvious claims 10-14.

G. The combination of *Lewis, Jain*, and *Owens* fails to render obvious claims 10-14 because the combination of *Lewis, Jain*, and *Owens* fails to disclose that the PSL router assigns a label for the return LSP.

In addition to the reasons provided above, the combination of *Lewis*, *Jain*, and *Owens* fails to render obvious claims 10-14 because the combination of *Lewis*, *Jain*, and *Owens* fails to disclose that the PSL router assigns a label for the return LSP. Claim 10 reads:

> 10. The method according to claim 9, after the PML router receives the notification message, if it is determined that the protection is in the 1:1 mode and it is chosen to create the return LSP dynamically via signaling, further comprising:
>
> the PML router transmitting to the PSL router a third message of requesting for creating the return LSP, with the binding information included in the third message;
>
> **the PSL router assigning a label for the return LSP** according to the third message, and returning a fourth message which comprises the binding information;
>
> the PML router binding the work LSP and the return LSP based on the binding information of the fourth message, and transmitting to the PSL router a notification message which comprises the binding information; the PSL router binding the work LSP and the return LSP based on the binding information of the notification message.

(Emphasis added). As shown above, claim 10 requires that the PSL router assigns a label for the return LSP. The Examiner contends that *Owens's* col. 1, ll. 40-46 disclose that the PSL router assigns a label for the return LSP. *See Examiner's Answer*, p. 24. However, the cited sections of *Owens's* disclose assigning labels to IP packets, not assigning a label to the return LSP:

> The key concept in MPLS is identifying and marking IP packets with labels and forwarding them to a modified switch or router, which then uses the labels to switch the packets through the network. The labels are created and assigned to IP packets based upon the information gathered from existing IP routing protocols.

Owens, col. 1, ll. 41-46. As shown above, *Owens* assigns labels to IP packets, but does not disclose assigning a label to the return LSP by the PSL router. *Lewis* and *Jain* fail to make up for the shortcomings of *Owens*. Thus, the combination *Lewis*, *Jain*, and *Owens* fails to disclose that the PSL router assigns a label for the return LSP. As such, the combination of *Lewis*, *Jain*, and *Owens* fails to disclose all of the elements of claim 10, and consequently, fails to render obvious claims 10-14.

IV. CONCLUSION

In view of the above arguments, the Appellants respectfully request that the rejection of the claims be reversed and the case advanced to issue. If the Examiner feels that a telephone interview would advance prosecution of the instant application, then the Appellants invite the Examiner to call the attorneys of record.

The Commissioner is hereby authorized to charge payment of any further fees associated with any of the foregoing papers submitted herewith, or to credit any overpayment thereof, to Deposit Account No. 50-1515, of Conley Rose, P.C. of Texas.

Respectfully submitted,
CONLEY ROSE, P.C.

Date: 6/24/11

Grant Rodolph

Grant Rodolph
Reg. No. 50,487

ATTORNEY FOR APPELLANT

5601 Granite Parkway, Suite 750
Plano, Texas 75024
Telephone: (972) 731-2288
Facsimile: (972) 731-2289